Making a Career in Network Security

Design it. Defend it. Monitor it. The network security career explained.

AUTHOR	Babashaheer
VERSION	1.0
DATE	April 2026
SERIES	Cybersecurity Career Series — Document 05 of 09
AUDIENCE	Students and professionals considering a network security career

Contents

1. What Is Network Security?

Every piece of data your organisation sends or receives travels across a network. Every employee, device, server and application is connected. Network security is the discipline of controlling what is allowed to travel across those connections — and detecting and stopping what is not.

It is one of the oldest and most operationally critical areas of cybersecurity. Long before cloud computing and application security became prominent disciplines, network security was already a core concern. Today it has evolved to cover not just physical network infrastructure but cloud networking, SD-WAN, remote access, IoT device connectivity and zero trust architectures.

> **Network security is fundamentally about controlling traffic.**
> Who can talk to whom. From where. Using which protocols. At what times.
> Everything else — monitoring, detection, response — builds on getting that right.

The scale of the problem

Verizon's 2023 Data Breach Investigations Report found that network-level attacks — including exploitation of public-facing applications and use of stolen credentials for remote access — were involved in the majority of breaches. The UK Government's Cyber Security Breaches Survey (DSIT, 2024) found that 50% of UK businesses experienced a cyber incident in the past year, with network intrusion the most common vector for significant attacks.

Level	Typical UK Salary	Common Roles
Junior	£26,000 – £40,000	Network Security Analyst, NOC Engineer, Junior SOC
Mid-level	£45,000 – £65,000	Network Security Engineer, Firewall Engineer, IR Analyst
Senior	£65,000 – £90,000+	Lead Network Security Architect, Senior Security Engineer
Specialist / Contractor	£400 – £900/day	Network Security Consultant, Zero Trust Architect

Table 1: UK salary ranges for network security roles (CW Jobs, 2024)

2. Network Security vs Other Cybersecurity Roles

Network security overlaps with several other cybersecurity disciplines. Understanding what makes it distinct — and where it connects — helps you decide if this is the right path.

	Network Security	Ethical Hacking	SOC / Blue Team	DFIR
Primary focus	Designing and enforcing traffic controls	Finding exploitable weaknesses	Detecting live threats	Investigating past incidents
Mindset	Architect / Defender	Attacker	Analyst / Responder	Investigator
Is it proactive?	Yes — design comes first	Yes — tests defences	Reactive — responds to alerts	Reactive — post-incident
Main tools	Firewalls, IDS/IPS, Wireshark	Nmap, Metasploit, Burp	SIEM, EDR, playbooks	FTK, Volatility, logs
Entry point	Network+ / CCNA then security overlay	CEH / eJPT / TryHackMe	Security+ / SOC Level 1	Security+ / BTL1
Suits people who	Enjoy infrastructure and architecture	Enjoy breaking things	Enjoy alert triage and process	Enjoy investigative work

Table 2: Network security compared to other cybersecurity disciplines

3. The Defence-in-Depth Model

No single security control stops every attack. Defence-in-depth is the principle of layering multiple independent controls so that if one layer fails, the next one catches the attacker. Network security sits at multiple layers of this model — from the perimeter firewall all the way through to internal network segmentation.

Defence-in-Depth — Layered Network Security Model

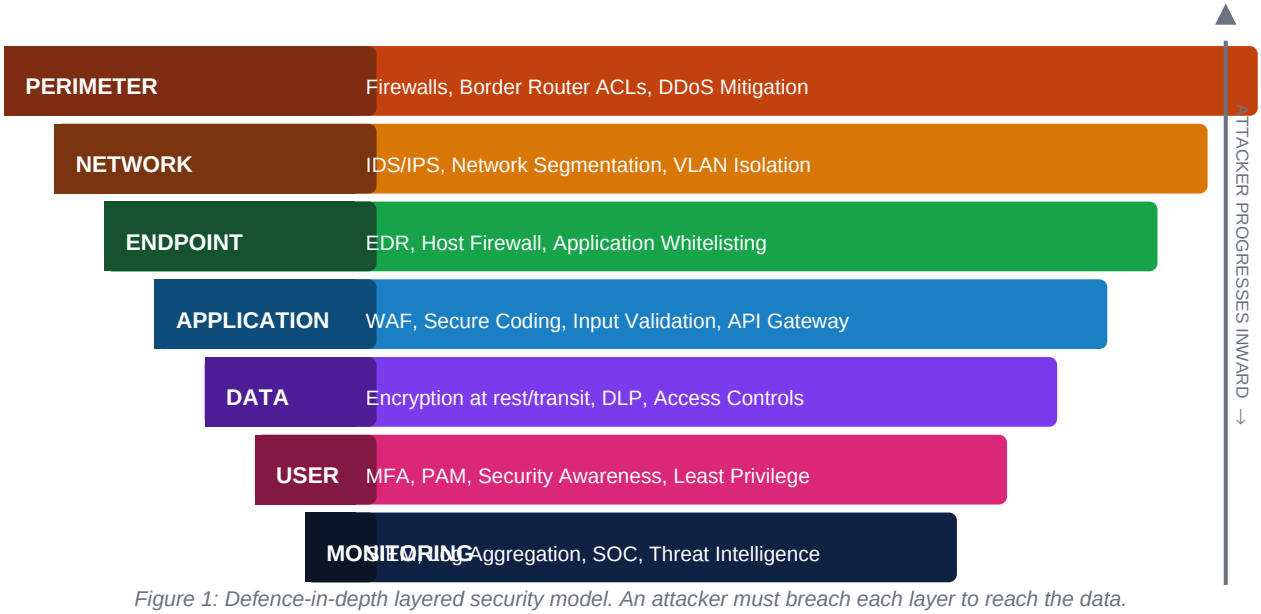


Figure 1: Defence-in-depth layered security model. An attacker must breach each layer to reach the data.

Network security professionals own the top two layers — perimeter and network — and contribute significantly to the endpoint and monitoring layers. Understanding where your controls sit and what happens when they fail is core to good network security design.

4. What a Network Security Professional Does

Network security is predominantly an operational and engineering discipline. Unlike penetration testers who work on engagements, or forensic analysts who respond to incidents, network security professionals often work in long-running operational roles maintaining, tuning and improving the same infrastructure over months and years.

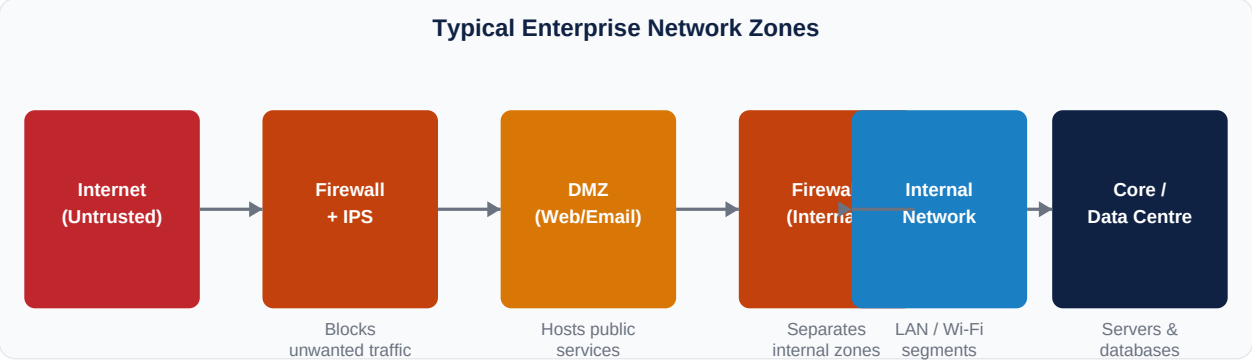


Figure 2: Typical enterprise network zone diagram. Network security professionals design and own each boundary.

Activity	% of Time	What This Looks Like
Firewall rule management	20–25%	Reviewing, writing and auditing firewall rules. Removing stale rules. Change management.
IDS/IPS tuning	15–20%	Reviewing alerts, reducing false positives, writing new detection signatures.
Network monitoring	20–25%	Watching traffic dashboards, reviewing flow data, investigating anomalies.
Architecture and design	15–20%	Planning segmentation changes, new VLAN designs, Zero Trust implementation projects.
Incident response (network)	10–15%	Isolating compromised segments, blocking attacker IPs, supporting the SOC.
Documentation and compliance	10%	Keeping network diagrams up to date, audit evidence, firewall rule review reports.

Table 3: Typical time split for a network security engineer

5. Core Technical Concepts You Must Know

Network security is built on top of networking fundamentals. If you do not understand how traffic works, you cannot understand how to control or detect attacks. The concepts below are non-negotiable — every network security role assumes competence in all of them.

5.1 TCP/IP and the OSI Model

Every attack and every defence maps to one or more layers of the network stack. A port scan operates at layer 4 (Transport). ARP spoofing operates at layer 2 (Data Link). HTTP injection operates at layer 7 (Application). Understanding which layer an attack targets tells you which control defends against it.

OSI Layer	Protocol Examples	Common Attack	Network Security Control
7 — Application	HTTP/S, DNS, SMTP, FTP	SQL injection, XSS, phishing	WAF, application proxy, DLP
6 — Presentation	SSL/TLS, JPEG, MPEG	SSL stripping, weak cipher exploit	TLS inspection, cipher policy
5 — Session	NetBIOS, RPC, PPTP	Session hijacking	Stateful firewall, session timeout
4 — Transport	TCP, UDP	Port scanning, SYN flood	Firewall ACLs, rate limiting, IPS
3 — Network	IP, ICMP, OSPF, BGP	IP spoofing, route injection	Router ACLs, RPF, BGP filtering
2 — Data Link	Ethernet, ARP, 802.1Q	ARP spoofing, VLAN hopping	Dynamic ARP Inspection, port security
1 — Physical	Cables, hubs, wireless	Physical tap, rogue AP	Physical access controls, 802.1X NAC

Table 4: OSI model — attacks and controls at each layer

5.2 Firewalls

Firewalls are the foundation of network security. Understanding the different types and when each is appropriate is fundamental knowledge for any role in this field:

- **Packet filter (stateless):** Inspects each packet in isolation against source/destination IP and port rules. Fast but limited — cannot track connection state.
- **Stateful firewall:** Tracks the state of connections. Knows whether a packet is part of an established session or a new connection attempt. The basis of most modern firewall rules.
- **Next-Generation Firewall (NGFW):** Adds application awareness, user identity, intrusion prevention, SSL inspection and threat intelligence feeds on top of stateful inspection. Vendors: Palo Alto, Fortinet, Check Point, Cisco Firepower.
- **Web Application Firewall (WAF):** Specifically designed for HTTP/S traffic. Detects OWASP Top 10 attacks. Sits in front of web applications, not the whole network.

5.3 IDS and IPS

An Intrusion Detection System (IDS) monitors traffic and generates alerts when it sees patterns matching known attacks. An Intrusion Prevention System (IPS) does the same but also takes action — blocking the traffic automatically. The distinction matters for deployment decisions: IPS tuning is critical because a misconfigured IPS that blocks legitimate traffic will cause outages.

Type	Detection Method	Response	Examples
Signature-based	Matches traffic against known attack patterns (like antivirus)	Alert or block	Snort, Suricata, Cisco IPS
Anomaly-based	Builds a baseline of normal traffic and alerts on deviation	Alert (mostly)	Darktrace, Vectra, Zeek
Heuristic	Uses rules derived from attack behaviour patterns	Alert or block	Modern NGFW built-in IPS
Network-based (NIDS)	Monitors traffic across the whole network	Alert	Snort, Zeek, Security Onion
Host-based (HIDS)	Monitors traffic and activity on a specific endpoint	Alert or block	OSSEC, Wazuh

Table 5: IDS and IPS types compared

5.4 VPNs, NAC and Network Segmentation

- **VPN (Virtual Private Network):** Encrypts traffic between a remote user or site and the corporate network. IPsec and SSL/TLS VPNs are most common. Know the difference between site-to-site and client-to-site VPNs.
- **Network Access Control (NAC):** Ensures that only authorised and compliant devices can connect to the network. Uses 802.1X for wired and wireless authentication. Cisco ISE and Aruba ClearPass are the leading enterprise platforms.
- **VLANs and Segmentation:** Separating a flat network into isolated segments. If an attacker compromises a machine in the Sales VLAN, segmentation prevents them from reaching the Finance VLAN without crossing a firewall.
- **Microsegmentation:** Fine-grained segmentation down to the workload or application level. Common in cloud and data centre environments. Central to Zero Trust architectures.

6. Zero Trust — The Modern Network Model

Traditional network security operated on a castle-and-moat model: everything inside the perimeter was trusted, everything outside was not. That model broke down completely when remote working, cloud services and BYOD devices made the 'inside' impossible to define. Zero Trust replaces it with a simple principle:

> **"Never trust, always verify."**
> No user, device or network segment is trusted by default — regardless of location.
> Every access request must be authenticated, authorised and continuously validated.

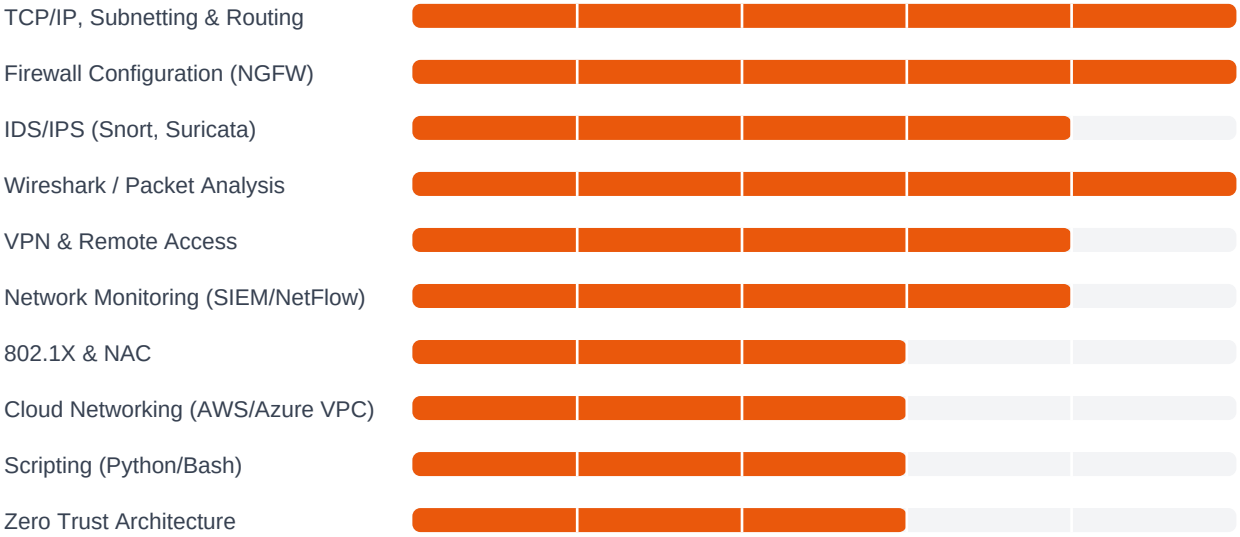
Zero Trust Principle	What It Means in Practice	Technology Used
Verify explicitly	Every access request requires identity verification — MFA, device health check, context	Identity providers (Azure AD, Okta), MFA, Conditional Access
Use least privilege access	Users and systems get only the minimum access needed for their specific task	PAM, RBAC, Just-in-Time access, microsegmentation
Assume breach	Design as if the attacker is already inside — segment everything, monitor everything	SIEM, EDR, microsegmentation, network monitoring
Continuous validation	Trust is not granted once — it is re-evaluated for every session and request	CASB, continuous authentication, behavioural analytics
Inspect all traffic	Encrypt all traffic — then inspect it. Nothing passes without inspection	TLS inspection, NGFW, DNS security

Table 6: Zero Trust principles and their practical implementation

Zero Trust is not a product you buy — it is an architecture you build over time. Understanding it is increasingly mandatory for senior network security roles. The UK National Cyber Security Centre (NCSC) and NIST both publish Zero Trust architecture guidance that is worth studying directly (NCSC, 2023; NIST, 2020).

7. Core Skills and Tools

Skill depth expected in a mid-level network security role:



Tool / Platform	Category	What It Does	Cost
Wireshark	Packet Analysis	Deep packet inspection. Read pcap files, analyse protocols, spot anomalies.	Free
Snort	IDS/IPS	Open-source rule-based intrusion detection. Write custom rules to detect specific attacks.	Free
Suricata	IDS/IPS	Multi-threaded IDS/IPS with Snort rule compatibility. More performant than Snort at high traffic volumes.	Free
Zeek (formerly Bro)	Network Monitor	Extracts metadata from network traffic — connections, DNS, HTTP, files — in structured logs.	Free
Nmap	Scanning	Network discovery and port scanning. Used both by defenders (asset discovery) and attackers.	Free
pfSense / OPNsense	Firewall	Open-source firewall platforms with full NGFW features. Excellent for lab environments.	Free
Security Onion	NSM Platform	All-in-one network security monitoring: Zeek + Suricata + Elasticsearch + Kibana.	Free
Palo Alto PAN-OS	NGFW	Enterprise NGFW. Understanding PAN-OS configuration is a strong differentiator for senior roles.	Commercial
Cisco IOS / NX-OS	Network OS	Cisco CLI for routers and switches — ACLs, routing security, port security, 802.1X.	Commercial
Darktrace	AI-based IDS	Behavioural anomaly detection using machine learning. Builds a 'pattern of life' per device.	Commercial

Tool / Platform	Category	What It Does	Cost
SolarWinds / PRTG	Network Monitor	Network performance and availability monitoring. Often integrated with security workflows.	Commercial

Table 7: Core tools for network security professionals

8. Career Paths in Network Security

Network security offers a wide range of career directions — from hands-on engineering and operations to architecture and consulting. Many network security professionals start as network engineers or administrators and add security specialisation over time.

Role	What You Do	Where You Work	UK Salary
Network Operations Centre (NOC) Engineer	Monitor network performance and availability. First line for network incidents.	Telecoms, ISPs, enterprises	£22k–£35k
Network Security Analyst	Analyse firewall logs, IDS alerts and network traffic. Investigate anomalies.	Corporate IT, MSSP	£30k–£50k
Firewall Engineer	Manage firewall rule sets across multiple platforms. Change management, auditing.	Enterprises, MSSPs	£35k–£55k
Network Security Engineer	Design and implement network security controls — firewalls, IPS, NAC, VPN, segmentation.	Enterprises, consultancies	£45k–£70k
Security Operations Engineer	Build and run network monitoring and detection infrastructure. SIEM, NDR, NetFlow.	Large enterprises, SOC teams	£45k–£70k
Network Security Architect	Design the overall network security strategy. Zero Trust planning, cloud migration security.	Large enterprises, consulting firms	£70k–£100k+
Network Security Consultant	Independent advisory and implementation work across multiple clients.	Self-employed, boutique firms	£500–£900/day

Table 8: Career paths in network security (Reed, 2024; CW Jobs, 2024)

Most network security engineers start as network engineers.
A CCNA followed by Security+ is the most common entry path into this field.
Adding a security overlay to networking skills is faster than learning networking from scratch.

9. The Learning Roadmap

Network security has a clearer foundational path than most cybersecurity disciplines. Start with networking. Build security on top of it. You cannot configure or defend a network you do not understand.

1. **Master TCP/IP and subnetting**
   Understand how IP addressing works — subnetting, CIDR, routing between networks. Know the OSI model and which protocols operate at each layer. Professor Messer's Network+ course is free and thorough. 4–6 weeks.

2. **Get hands-on with a lab**
   Install GNS3 or Cisco Packet Tracer (both free). Build a simple network — router, switch, firewall, two VLAN segments. Practice routing, ACLs and basic firewall rules. Build the topology in Figure 2 from memory. 4–6 weeks.

3. **Learn Wireshark deeply**
   Capture traffic from your lab. Learn to filter by protocol, follow TCP streams, spot ARP anomalies and identify unencrypted credentials. The Wireshark University course is free and excellent. This skill is tested in almost every interview. 2–3 weeks.

4. **Study IDS/IPS with Snort and Suricata**
   Install Security Onion (free, all-in-one). Run Suricata against captured traffic and learn to read and write Snort rules. Understanding how detection works at the rule level is essential. 3–4 weeks.

5. **Build firewall lab skills**
   Install pfSense or OPNsense in a VM (free). Configure NAT, ACLs, VLAN interfaces and basic IPS. If you can access Palo Alto PANOS in a lab, even better. Many vendors offer free virtual firewall labs. 3–4 weeks.

6. **Study for CompTIA Network+**
   Structures and validates all the foundational knowledge above. Professor Messer's free course + practice exams. Even if you do not sit it, the curriculum is the map of what you need to know. 4–6 weeks.

7. **Get Security+ and Cisco CCNA**
   Security+ validates broad security knowledge. CCNA validates network engineering competence. Together they are the most common entry combination for junior network security roles in the UK.

8. **Add cloud networking knowledge**
   Learn AWS VPC or Azure Virtual Network — security groups, NACLs, ExpressRoute. Cloud networking is now inseparable from on-premise network security. AWS free tier gives you a real environment to practice. Ongoing.

Realistic timeline from zero to junior role: 12–18 months.
If you already have a networking background: 6–9 months to add the security overlay.

10. Certifications That Matter

Network security certifications span both the networking and security stacks. The most respected path combines a vendor-neutral networking cert (Network+), a vendor-neutral security cert (Security+), and a hands-on vendor or specialist cert (Cisco, Palo Alto or GIAC).

Certification	Level	Who Awards It	Why It Matters
CompTIA Network+	Beginner	CompTIA	Validates core networking knowledge. Required baseline for most network roles.
CompTIA Security+	Beginner	CompTIA	Validates broad security foundations. Required for many UK government and defence network roles.
Cisco CCNA	Beginner–Mid	Cisco	The most recognised networking qualification globally. Covers routing, switching and basic security.
Cisco CCNA Security / CyberOps	Mid	Cisco	Specialises CCNA into firewall, VPN and security monitoring. Well regarded by enterprise employers.
PCNSA — Palo Alto	Mid	Palo Alto Networks	Professional-level certification for PAN-OS firewall administration. Highly valued for firewall engineer roles.
Fortinet NSE 4–7	Mid–Senior	Fortinet	Vendor certification for FortiGate. Fortinet is the market leader in SME/enterprise firewall deployments in UK.
GCIA — GIAC Certified Intrusion Analyst	Mid	GIAC / SANS	Deep network traffic analysis and intrusion detection. Highly respected for network monitoring and SOC roles.
GCFW — GIAC Certified Firewall Analyst	Mid	GIAC / SANS	Firewall architecture, policy and management. One of the best specialist certs for senior firewall roles.
CCNP Security	Senior	Cisco	Advanced Cisco security — enterprise firewall, VPN, identity, secure access.

Table 9: Certifications for network security professionals, ordered by progression

11. Case Study — Stopping an Intrusion at the Perimeter

> This is a fictional case study based on common real-world network intrusion patterns.
> It shows how a network security engineer detects, analyses and responds to a perimeter threat.

The Organisation

Harlow Financial Services is a UK-based investment firm with 150 staff. They run an on-premise data centre with financial application servers and a cloud-hosted customer portal. Their network has a perimeter NGFW, an IPS, and a SIEM fed by firewall and Windows event logs. The network security engineer, James, works a normal Monday morning.

08:47 — An IPS alert

08:47 — Suricata IPS Alert: ET SCAN Nmap Scripting Engine

James receives an IPS alert: a single external IP (185.220.101.47) is running an aggressive Nmap scan against the company's public IP range — probing ports 22, 80, 443, 3389 and 8080 in rapid succession.

First action: James queries the SIEM for any previous activity from this IP. It first appeared 6 days ago with low-and-slow port probes that did not trigger any alerts. Today it switched to aggressive scanning — a common pattern

09:05 — Correlation and threat intelligence

09:05 — Threat Intel Lookup

James queries the IP against three threat intelligence feeds: AbuseIPDB, VirusTotal and AlienVault OTX. The IP is flagged across all three as a known Tor exit node associated with scanning and brute-force activity.

Port 3389 (RDP) is receiving the most probe traffic. James checks the firewall rule set — RDP is permitted inbound for a small number of legacy systems that use it for remote administration. This is a known risk that has been on the

09:22 — Active blocking and rule creation

09:22 — Firewall block + IPS rule update

James creates a geo-block rule on the perimeter NGFW to drop all traffic from known Tor exit node IP ranges — a list maintained by the Tor Project and updated daily. The specific IP is also added to the manual block list.

He then creates a custom IPS rule to alert and block any traffic matching the Nmap scripting engine user agent or scan pattern. The block is logged in the SIEM with a ticket reference for audit trail purposes.

10:15 — Root cause and remediation

The scan revealed an underlying problem: RDP should not be open at the perimeter at all. James documents the remediation recommendation formally:

- Immediately disable inbound RDP at the perimeter firewall for all external IPs
- Require all remote access via the corporate VPN with MFA — remove direct RDP exposure
- Enable Account Lockout Policy on all systems accepting RDP to prevent brute force
- Subscribe to a commercial threat intelligence feed to receive Tor exit node IP updates automatically
- Schedule a quarterly firewall rule review — the open RDP rule was three years old

Time	Event	Detection Source	Action
Mon–Fri prior	Low-and-slow port probes	Not detected — below threshold	None (missed)
08:47 Mon	Aggressive Nmap scan begins	Suricata IPS rule	Alert generated
09:05	Threat intel lookup	SIEM + TI feeds	IP classified as malicious
09:22	Scanning continues	IPS block rule created	Traffic blocked
09:30	Attack traffic stopped	Firewall confirm zero hits	Block confirmed effective
10:15	Remediation report submitted	Manual review	RDP closure recommended

Table 10: Timeline of the Harlow Financial Services network intrusion attempt

The open RDP port had been there for three years.
No regular firewall rule review. No automatic threat intel blocking. No VPN policy.
All three gaps are standard baseline controls — and all three were absent.

12. Breaking In — Getting Your First Role

Network security roles are often filled internally — network engineers who add security knowledge are a natural fit. If you are starting from outside the networking world, your clearest path is to get a junior network role first, then transition.

Build visible evidence of skill

- **GNS3 / Packet Tracer lab:** Build a segmented network with a firewall, IDS and multiple VLANs. Document it. Put the configuration on GitHub. Employers want to see you have done this
- **Security Onion home lab:** Install Security Onion on an old PC or VM, feed it traffic, learn to navigate the Kibana dashboards and write Suricata rules. Document your setup
- **TryHackMe and Hack The Box (Blue Team paths):** Complete the SOC Analyst path which includes significant network analysis content. Your profile shows completion
- **Wireshark University / PCAP analysis:** Download public packet captures from malware-traffic-analysis.net and practice identifying malicious activity. Write up your analysis
- **CTF competitions:** Network forensics challenges at CTFtime.org involve pcap analysis, firewall rule puzzles and protocol analysis — good for demonstrating practical skills

Where to Look	Notes
CyberSecurityJobs.com	Filter by 'network security analyst', 'firewall engineer'
LinkedIn	Network security roles post heavily here. Connect with firewall engineers and CISO contacts
Cisco Jobs / Palo Alto careers	Vendor-side roles often require less experience if you hold their certs
Public sector / NHS / HMRC	UK government network security roles are plentiful and often accept junior applicants with Network+ and Security+
MSSPs (Managed Security Service Providers)	MSSP NOC and security analyst roles are excellent entry points with heavy exposure to diverse client environments

Table 11: Where to find network security roles

Interview questions to prepare for

- What is the difference between a stateful and a stateless firewall?
- Explain the three-way TCP handshake. What does a half-open connection tell you?
- What would you look for in a packet capture to detect a port scan?
- What is a VLAN and why does it improve security compared to a flat network?
- Walk me through how you would respond to an IPS alert for outbound C2 traffic.
- What is the difference between IDS and IPS? When would you use each?
- What is Zero Trust and how does it differ from perimeter-based security?
- How do you prevent VLAN hopping attacks?

The best answer in a network security interview:
"Here is my lab. Here is the topology I built. Here is the firewall rule I wrote."
Practical evidence of hands-on lab work consistently beats theory alone.

13. References

1. Cisco (2024) *Cisco CCNA Certification Overview.* Available at: https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna.html [Accessed: 10 April 2026].

2. CW Jobs (2024) *Technology Salary Survey 2024.* Available at: https://www.cwjobs.co.uk/salary-checker [Accessed: 10 April 2026].

3. DSIT (2024) *Cyber Security Breaches Survey 2024.* Department for Science, Innovation and Technology. Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024 [Accessed: 11 April 2026].

4. Fortinet (2024) *NSE Certification Programme.* Available at: https://training.fortinet.com/local/staticpage/view.php?page=nse_institute [Accessed: 11 April 2026].

5. GIAC (2024) *GCIA and GCFW Certification Overview.* Available at: https://www.giac.org/certifications/network-security [Accessed: 11 April 2026].

6. NCSC (2023) *Zero Trust Architecture Design Principles.* National Cyber Security Centre. Available at: https://www.ncsc.gov.uk/collection/zero-trust-architecture [Accessed: 12 April 2026].

7. NIST (2020) *Zero Trust Architecture (SP 800-207).* National Institute of Standards and Technology. Available at: https://doi.org/10.6028/NIST.SP.800-207 [Accessed: 12 April 2026].

8. Palo Alto Networks (2024) *PCNSA Certification.* Available at: https://www.paloaltonetworks.com/services/education/certification [Accessed: 12 April 2026].

9. Reed (2024) *Cybersecurity Salary Guide UK 2024.* Available at: https://www.reed.co.uk/career-advice/cybersecurity-salary [Accessed: 13 April 2026].

10. Verizon (2023) *Data Breach Investigations Report 2023.* Available at: https://www.verizon.com/business/resources/reports/dbir/ [Accessed: 13 April 2026].

Document prepared by **Babashaheer**. Version 1.0 — April 2026. Cybersecurity Career Series — Document 05 of 09.